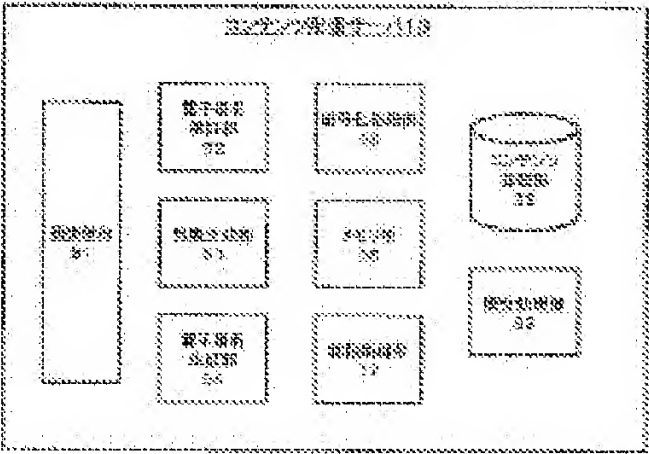


MUTUAL AUTHENTICATION SYSTEM, MUTUAL AUTHENTICATION METHOD, MUTUAL AUTHENTICATION EQUIPMENT AND STORAGE MEDIUM

**Publication number:** JP2003124927 (A)  
**Publication date:** 2003-04-25  
**Inventor(s):** ISHIGURO RYUJI; TADA KEIKO +  
**Applicant(s):** SONY CORP +  
**Classification:**  
- international: *G06F15/00; G06F21/20; G06Q10/00; G06Q30/00; G06Q50/00; H04L9/32; G06F15/00; G06F21/20; G06Q10/00; G06Q30/00; G06Q50/00; H04L9/32;*  
(IPC1-7): G06F15/00; G06F17/60; H04L9/32  
- European:  
**Application number:** JP20010317328 20011015  
**Priority number(s):** JP20010317328 20011015

**Abstract of JP 2003124927 (A)**  
**PROBLEM TO BE SOLVED:** To perform mutual authentication by using NTRU public key encryption method. **SOLUTION:** Mutual authentication between a server and a client is performed with the protocol using an NTRU private key encryption method. By adding random numbers which are going to be seeds of a session key and their hash value to transmission data, it makes possible to check whether description failure is generated. The session key is formed on the basis of the random numbers for the session key, and data transmission and reception after authentication are performed by encryption. Process of the NTRU encryption method is light and the protocol is simple, so that mounting to an assembly type apparatus is enabled.

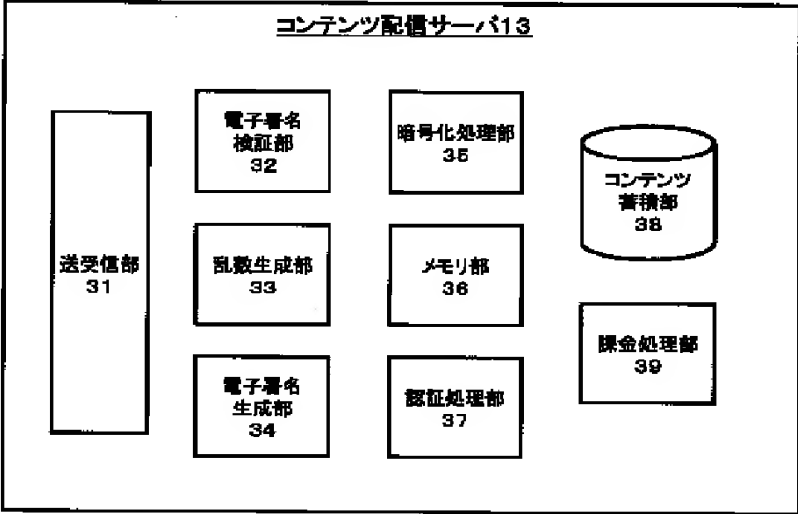


(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)	
H 0 4 L 9/32		G 0 6 F 15/00	3 3 0 C	5 B 0 8 5
G 0 6 F 15/00	3 3 0	17/60	3 0 2 E	5 J 1 0 4
17/60	3 0 2		3 3 2	
	3 3 2		5 1 2	
	5 1 2		Z E C	
審査請求 未請求 請求項の数20 O L （全 15 頁） 最終頁に続く				

(21)出願番号	特願2001－317328(P2001－317328)	(71)出願人	000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22)出願日	平成13年10月15日(2001.10.15)	(72)発明者	石黒 隆二 東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(72)発明者	多田 恵子 東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(74)代理人	100101801 弁理士 山田 英治 (外2名)
		最終頁に続く	

(54)【発明の名称】 相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体

(57)【要約】  
【課題】 N T R U公開鍵暗号方式を使用して相互認証を行う。  
【解決手段】 N T R U公開鍵暗号方式を用いたプロトコルによりサーバとクライアント間の相互認証を行う。また、送信データ中にセッション・キーの種となる乱数とそのハッシュ値を加えることにより、D e c r i p t i o n F a i l u r eが起きているかどうかをチェックできるようするとともに、セッション・キー用の乱数を基にセッション・キーを作り出して、認証後のデータ送受信を暗号化して行う。N T R Uの暗号化方式は処理が軽く簡単なプロトコルであることから、組み込み型機器に実装することが可能である。



## 【特許請求の範囲】

【請求項 1】通信媒体を介して接続される複数の装置間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証システムであって、

通信相手が互いにセッション・キーの種となる乱数を生成するセッション・キーの種生成手段と、

相互認証用のデータ中にセッション・キーの種となる乱数とそのハッシュ値を付加することによって、復号化の失敗が起きているかどうかをチェックする復号化検査手段と、を備えることを特徴とする相互認証システム。

【請求項 2】前記公開鍵暗号方式は、NTRU 公開鍵暗号方式である、ことを特徴とする請求項 1 に記載の相互認証システム。

【請求項 3】前記復号化検査手段は、通信相手の公開鍵でセッション・キーの種となる乱数とそのハッシュ値を暗号化して送信するとともに、通信相手から受信したデータを自分の秘密鍵で復号化して、セッション・キーの種となる乱数とそのハッシュ値を取り出し、セッション・キーの種となる乱数のハッシュ値を算出してこれを取り出された該ハッシュ値と比較することによって、公開鍵における復号化に失敗したか否かを判別する、ことを特徴とする請求項 1 に記載の相互認証システム。

【請求項 4】通信相手が互いに生成したセッション・キーの種を基にセッション・キーを生成するセッション・キー生成手段と、

該セッション・キーを用いた暗号データの送受信を行う暗号データ送受信手段と、

をさらに備えることを特徴とする請求項 1 に記載の相互認証システム。

【請求項 5】通信媒体を介して接続される複数の装置間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証方法であって、

通信相手が互いにセッション・キーの種となる乱数を生成するセッション・キーの種生成ステップと、

相互認証用のデータ中にセッション・キーの種となる乱数とそのハッシュ値を付加することによって、復号化の失敗が起きているかどうかをチェックする復号化検査ステップと、を備えることを特徴とする相互認証方法。

【請求項 6】前記公開鍵暗号方式は、NTRU 公開鍵暗号方式である、ことを特徴とする請求項 5 に記載の相互認証方法。

【請求項 7】前記復号化検査ステップでは、通信相手の公開鍵でセッション・キーの種となる乱数とそのハッシュ値を暗号化して送信するとともに、通信相手から受信したデータを自分の秘密鍵で復号化して、セッション・キーの種となる乱数とそのハッシュ値を取り出し、セッション・キーの種となる乱数のハッシュ値を算出してこれを取り出された該ハッシュ値と比較することによって、公開鍵における復号化に失敗したか否かを判別する、ことを特徴とする請求項 5 に記載の相互認証方法。

【請求項 8】通信相手が互いに生成したセッション・キーの種を基にセッション・キーを生成するステップと、該セッション・キーを用いた暗号データの送受信を行うステップと、をさらに備えることを特徴とする請求項 5 に記載の相互認証方法。

【請求項 9】第 1 の装置と第 2 の装置の間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証方法であって、

第 1 の装置が自分の公開鍵  $E_a$  を含んだ電子署名  $C_a$  を第 2 の装置に送信するステップと、

第 2 の装置が、第 1 の装置の電子署名  $C_a$  を確認した後、相互認証用の乱数  $N_b$  及びセッション・キーの種  $S_b$  を生成するとともに  $S_b$  のハッシュ値  $Hash(S_b)$  を計算して、 $N_b$ 、 $S_b$ 、 $Hash(S_b)$  を第 1 の装置の公開鍵  $E_a$  で暗号化したデータ  $E_a(N_b, S_b, Hash(S_b))$  を、自分の公開鍵  $E_b$  を含んだ電子署名  $C_b$  とともに第 1 の装置に送信するステップと、

第 1 の装置が、第 2 の装置の電子署名  $C_b$  を確認した後、自分の秘密鍵で受信データ  $E_a(N_b, S_b, Hash(S_b))$  を復号化して、セッション・キーの種  $S_b$  のハッシュ値  $Hash'(S_b)$  を計算して、受信したハッシュ値  $Hash(S_b)$  と一致するか否かによって、公開鍵における復号化に失敗したか否かを判別するステップと、

復号化に失敗していないことに応答して、第 1 の装置が、相互認証用の乱数  $N_a$  及びセッション・キーの種  $S_a$  を生成するとともに  $S_a$  のハッシュ値  $Hash(S_a)$  を計算して、 $N_a$ 、 $S_a$ 、 $Hash(S_a)$  を第 2 の装置の公開鍵  $E_b$  で暗号化したデータ  $E_b(N_a, S_a, Hash(S_a))$  を、受信データから取り出した乱数  $N_b$  とともに第 2 の装置に送信するステップと、

第 2 の装置が、受信した乱数  $N_b$  が自分で生成した乱数と等しいか否かで第 1 の装置を本人確認するステップと、

本人確認に成功したことに応答して、第 2 の装置が、自分の秘密鍵で受信データ  $E_b(N_a, S_a, Hash(S_a))$  を復号化して、セッション・キーの種  $S_a$  のハッシュ値  $Hash'(S_a)$  を計算して、受信したハッシュ値  $Hash(S_a)$  と一致するか否かによって、公開鍵における復号化に失敗したか否かを判別するステップと、

復号化に失敗していないことに応答して、第 2 の装置が、相互認証用の乱数  $N_a$  を第 1 の装置に送信するステップと、

第 1 の装置が、受信した乱数  $N_a$  が自分で生成した乱数と等しいか否かで第 2 の装置を本人確認するステップと、を具備することを特徴とする相互認証方法。

【請求項 10】前記公開鍵暗号方式は、NTRU 公開鍵暗号方式である、ことを特徴とする請求項 9 に記載の相互認証装置。

【請求項 1 1】第 1 及び第 2 の装置がそれぞれ互いに生成したセッション・キーの種  $S_a$  及び  $S_b$  を基にセッション・キーを生成するステップと、

第 1 及び第 2 の装置が該セッション・キーを用いた暗号データの送受信を行うステップと、をさらに備えることを特徴とする請求項 9 に記載の相互認証方法。

【請求項 1 2】通信媒体を介して接続される他の装置との間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証装置であって、

相互認証用の乱数  $N$  を発生する手段と、

セッション・キーの種となる乱数  $S$  を発生する手段と、

セッション・キーの種のハッシュ値  $H$  を計算する手段と、

乱数  $N$  とセッション・キーの種  $S$  とセッション・キーの種のハッシュ値  $H$  を通信相手の公開鍵で暗号化して送信する手段と、

通信相手から受信した暗号データを自分の公開鍵で復号化して、通信相手の相互認証用の乱数  $N'$  と通信相手が生成したセッション・キーの種  $S'$  及びそのハッシュ値  $H'$  を取り出す手段と、

セッション・キーの種  $S'$  のハッシュ値  $H''$  を計算して、 $H'$  と  $H''$  が一致するか否かによって公開鍵における復号化に失敗したか否かを検査する手段と、を具備することを特徴とする相互認証装置。

【請求項 1 3】前記公開鍵暗号方式は、NTRU 公開鍵暗号方式である、ことを特徴とする請求項 1 2 に記載の相互認証装置。

【請求項 1 4】通信相手から受信した暗号データから取り出した通信相手の相互認証用の乱数  $N'$  を通信相手に送信する手段と、

通信相手から受信した自分の相互認証用の乱数が、自分で発生した乱数  $N$  と等しいか否かで、通信相手を本人確認する手段と、をさらに備えることを特徴とする請求項 1 2 に記載の相互認証装置。

【請求項 1 5】自身で生成したセッションキーの種  $S$  及び他の装置から受信したセッションキーの種  $S'$  を基にセッション・キーを生成する手段と、

該セッション・キーを用いて他の装置との暗号データの送受信を行う手段と、をさらに備えることを特徴とする請求項 1 2 に記載の相互認証装置。

【請求項 1 6】他の装置との間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証方法であって、相互認証用の乱数  $N$  を発生するステップと、

セッション・キーの種となる乱数  $S$  を発生するステップと、

セッション・キーの種のハッシュ値  $H$  を計算するステップと、

乱数  $N$  とセッション・キーの種  $S$  とセッション・キーの種のハッシュ値  $H$  を通信相手の公開鍵で暗号化して送信するステップと、

通信相手から受信した暗号データを自分の公開鍵で復号化して、通信相手の相互認証用の乱数  $N'$  と通信相手が生成したセッション・キーの種  $S'$  及びそのハッシュ値  $H'$  を取り出すステップと、

セッション・キーの種  $S'$  のハッシュ値  $H''$  を計算して、 $H'$  と  $H''$  が一致するか否かによって公開鍵における復号化に失敗したか否かを検査するステップと、を具備することを特徴とする相互認証方法。

【請求項 1 7】前記公開鍵暗号方式は、NTRU 公開鍵暗号方式である、ことを特徴とする請求項 1 6 に記載の相互認証方法。

【請求項 1 8】通信相手から受信した暗号データから取り出した通信相手の相互認証用の乱数  $N'$  を通信相手に送信するステップと、

通信相手から受信した自分の相互認証用の乱数が、自分で発生した乱数  $N$  と等しいか否かで、通信相手を本人確認するステップと、をさらに備えることを特徴とする請求項 1 6 に記載の相互認証方法。

【請求項 1 9】自身で生成したセッションキーの種  $S$  及び他の装置から受信したセッションキーの種  $S'$  を基にセッション・キーを生成するステップと、

該セッション・キーを用いて他の装置との暗号データの送受信を行うステップと、をさらに備えることを特徴とする請求項 1 6 に記載の相互認証方法。

【請求項 2 0】他の装置との間で所定の公開鍵暗号方式を用いて相互認証を行うための相互認証処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、

相互認証用の乱数  $N$  を発生するステップと、

セッション・キーの種となる乱数  $S$  を発生するステップと、

セッション・キーの種のハッシュ値  $H$  を計算するステップと、

乱数  $N$  とセッション・キーの種  $S$  とセッション・キーの種のハッシュ値  $H$  を通信相手の公開鍵で暗号化して送信するステップと、

通信相手から受信した暗号データを自分の公開鍵で復号化して、通信相手の相互認証用の乱数  $N'$  と通信相手が生成したセッション・キーの種  $S'$  及びそのハッシュ値  $H'$  を取り出すステップと、

セッション・キーの種  $S'$  のハッシュ値  $H''$  を計算して、 $H'$  と  $H''$  が一致するか否かによって公開鍵における復号化に失敗したか否かを検査するステップと、を具備することを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、2 以上の機器間で相互認証システム及び相互認証方法、相互認証装置、並

びに記憶媒体に係り、特に、音楽や画像などの有料コンテンツの配信において課金処理時に相互認証を行う相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体に関する。

【0002】更に詳しくは、本発明は、公開鍵暗号方式を用いて相互認証を行う相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体に係り、特に、比較的処理が軽い公開鍵暗号方式を用いて携帯端末のような組み込み機器上でも相互認証を行うことができる相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体に関する。

【0003】

【従来の技術】昨今、情報通信技術の飛躍的な進歩とも相俟って、コンピュータを始めとする各種の情報機器が電話回線やインターネットなどの広域ネットワークに接続され、コンピュータ資源の共有や、情報の共有・流通・配布・交換などの協働的作業を円滑に行うことができるようになってきている。

【0004】ネットワークは、単なる情報配信の手段としてだけではなく、音楽や画像などの有料コンテンツの販売や、従来の物流に置き換わる「ネット販売」や「オンライン・ショッピング」にも活用されている。また、コンテンツや商品の購入手続だけではなく、電子マネーなどを利用して課金処理もネットワーク上で無人化・自動化することができる。

【0005】例えば、PDA(Personal Digital Assistant)のような携帯情報端末に携帯電話機を接続することにより、電話網やインターネット網を介してコンテンツをダウンロードすることによって、PDA上でコンテンツを再生して楽しむということができる。

【0006】他方、デジタル形式のデータやコンテンツの複製や改竄は極めて容易であり、著作権侵害の危険に無防備にさらされているとさえ言える。したがって、著作権法やその他の複製に関する法規制を強化するだけでは不十分であり、情報技術の観点からもデータやコンテンツの保護を拡充する必要があると史料される。

【0007】また、従来の物流とは相違し、ネットワーク取引においては、顔が見えない相手にコンテンツを渡したり対価を支払ったりしなければならず、コンテンツを無断複製や改竄などの海賊行為から保護したり、ユーザのプライバシーをなりすましによる侵害から充分に保護することが充分にできない可能性がある。

【0008】このため、ネットワーク世界では、正当な相手とのみ取引を行うべく、「相互認証」という手続が広く採り入れられている。

【0009】相互認証には、いわゆる「公開鍵暗号方式」を適用することが一般的である。ここで、公開鍵暗号とは、データを暗号化する際に用いる鍵と、復号化する際に用いる鍵が異なり、「非対称暗号」とも呼ばれる。公開鍵暗号アルゴリズムは、一方の鍵から他方の鍵

を算出することが非常に困難であるという性質を持つことにより、一方の鍵で暗号化した情報は他方の鍵でしか復号化できないことが保証される。暗号化の鍵は「公開鍵」と呼ばれ、一般に公開して誰でも使用できるようにする。また、復号化の鍵は「秘密鍵」と呼ばれ、他人に漏れないように所有者が管理する。

【0010】公開鍵暗号方式を採用した場合、各自は復号鍵として自分の秘密鍵を1つ所有するだけでよいので、システム全体で使用する鍵の数を少なくすることができ、管理が容易になる。

【0011】しかしながら、公開鍵暗号方式は、一般に、暗号化並びに復号化の処理が重たく、CPUパワーやメモリ容量を要する。量的にかなり小さい情報であれば、暗号化・復号化には実用上の支障はないが、音楽や画像などの比較的大きな情報の場合には支障が生じる。また、PDAのような小型（すなわちCPUパワーが非力）でバッテリー駆動の組み込み機器の場合には、相互認証に公開鍵暗号方式を用いるのは困難である。

【0012】しかしながら、もし、セッション・キー発生に使用される乱数などのデータが平文のまま通信路を流れると、通信路のデータが見られた場合には、それらの乱数を使って悪者がセッション・キーを簡単に作り出して、さまざまな不正を働く危険がある。

【0013】このような問題を解消するために、“NTRU(エヌトゥルー)”と呼ばれる、短く且つ用意に鍵を生成し、高速且つ小メモリ容量で実現可能な公開鍵暗号方式が開発・提供されている。

【0014】NTRUは世界で最も速く安全な公開鍵暗号システムであり、その処理速度は従来の公開鍵暗号システムと比べて20倍から400倍にも達する。また、NTRUは、システムの拡張が容易であり、頻繁なワイヤレス取引や音楽やゲームをダウンロードするために接続される数十億の消費者向けデバイスを保護するインフラストラクチャーの構築も可能である。一方、NTRUは低価格で大量に販売されるデバイスのセキュリティを、小さな構成で確実かつ効率的に守ることもできる。さらにNTRUは、新規のセキュリティ・パラダイムを使用して、付加価値の高いコミュニケーションとコンテンツのセキュリティを厳重に保護することもできる(<http://www.ntru.co.jp/>)。

【0015】NTRUは、因数分解や対数問題を使用しない、初の安全で実用的な公開鍵暗号システムである。NTRUのアルゴリズムを実行する計算プロセスは単純であるので、低価格の8ビット・マイクロプロセッサでも高速に処理することができる。すなわち、NTRUの公開鍵暗号方式は、比較的軽い処理で且つ小メモリ容量で実現できることから、携帯電話機、デジタル・ミュージック・プレーヤや、PDAなどのデバイスの使用時に、プライバシーと信頼性を確立することができると思料される。

【0016】しかしながら、NTRUは処理が軽い反面、復号化(Decryption)の際に基データが異なるというエラー(Decryption Failure)を発生することがある。

【0017】Decryption Failureが起こると、端末間で再度セッション確立などの手続を繰り返さなければならず、それまでに行われた相互認証などの処理がすべて無駄になってしまう。例えば、携帯電話などの機器からサーバに再接続しなければならず、処理時間だけでなく通信費も無駄になってしまう。

【0018】

【発明が解決しようとする課題】本発明の目的は、音楽や画像などの有料コンテンツの配信において課金処理時に相互認証を好適に行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することにある。

【0019】本発明の更なる目的は、公開鍵暗号方式を用いて機器間の相互認証を好適に行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することにある。

【0020】本発明の更なる目的は、比較的処理が軽い公開鍵暗号方式を用いて携帯端末のような組み込み機器上でも相互認証を行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することにある。

【0021】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第1の側面は、通信媒体を介して接続される複数の装置間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証システム又は相互認証方法であって、通信相手が互いにセッション・キーの種となる乱数を生成するセッション・キーの種生成手段又はステップと、相互認証用のデータ中にセッション・キーの種となる乱数とそのハッシュ値を付加することによって、復号化の失敗が起きているかどうかをチェックする復号化検査手段又はステップと、を備えることを特徴とする相互認証システム又は相互認証方法である。

【0022】但し、ここで言う「システム」とは、複数の装置(又は特定の機能を実現する機能モジュール)が論理的に集合した物のことを言い、各装置や機能モジュールが単一の筐体内にあるか否かは特に問わない。

【0023】本発明の第1の側面に係る相互認証システムは、CPUパワーが非力でメモリ容量が小さな携帯情報端末の相互認証を行うことを考慮して、NTRU公開鍵暗号方式を用いた相互認証処理を行う。

【0024】NTRU公開鍵暗号方式を用いた場合、復号化の失敗(Decryption Failure)が発生する可能性がある。そこで、本発明の第1の側面に係る相互認証システムでは、通信相手が互いにセッショ

ン・キーの種となる乱数を生成するとともに、相互認証用のデータ中にセッション・キーの種となる乱数とそのハッシュ値を付加することによって、復号化の失敗が起きているかどうかをチェックするようにした。この結果、確かなセッション確立でセッション・キーを共有することができる。

【0025】ここで、前記復号化検査手段又はステップは、通信相手の公開鍵でセッション・キーの種となる乱数とそのハッシュ値を暗号化して送信するとともに、通信相手から受信したデータを自分の秘密鍵で復号化して、セッション・キーの種となる乱数とそのハッシュ値を取り出し、セッション・キーの種となる乱数のハッシュ値を算出してこれを取り出された該ハッシュ値と比較することによって、公開鍵における復号化に失敗したか否かを判別することができる。

【0026】また、復号化の失敗が起きていないと判断された場合には、通信相手が互いに生成したセッション・キーの種を基にセッション・キーを生成して、該セッション・キーを用いた暗号データの送受信を行うことができる。すなわち、課金処理やコンテンツの配信などの手続を、安全な通信路を介して行うことが可能となる。

【0027】また、本発明の第2の側面は、第1の装置と第2の装置の間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証方法であって、第1の装置が自分の公開鍵 $E_a$ を含んだ電子署名 $C_a$ を第2の装置に送信するステップと、第2の装置が、第1の装置の電子署名 $C_a$ を確認した後、相互認証用の乱数 $N_b$ 及びセッション・キーの種 $S_b$ を生成するとともに $S_b$ のハッシュ値 $Hash(S_b)$ を計算して、 $N_b$ 、 $S_b$ 、 $Hash(S_b)$ を第1の装置の公開鍵 $E_a$ で暗号化したデータ $E_b(N_b, S_b, Hash(S_b))$ を、自分の公開鍵 $E_b$ を含んだ電子署名 $C_b$ とともに第1の装置に送信するステップと、第1の装置が、第2の装置の電子署名 $C_b$ を確認した後、自分の秘密鍵で受信データ $E_b(N_b, S_b, Hash(S_b))$ を復号化して、セッション・キーの種 $S_b$ のハッシュ値 $Hash'(S_b)$ を計算して、受信したハッシュ値 $Hash(S_b)$ と一致するか否かによって、公開鍵における復号化に失敗したか否かを判別するステップと、復号化に失敗していないことに応答して、第1の装置が、相互認証用の乱数 $N_a$ 及びセッション・キーの種 $S_a$ を生成するとともに $S_a$ のハッシュ値 $Hash(S_a)$ を計算して、 $N_a$ 、 $S_a$ 、 $Hash(S_a)$ を第2の装置の公開鍵 $E_b$ で暗号化したデータ $E_b(N_a, S_a, Hash(S_a))$ を、受信データから取り出した乱数 $N_b$ とともに第2の装置に送信するステップと、第2の装置が、受信した乱数 $N_b$ が自分で生成した乱数と等しいか否かで第1の装置を本人確認するステップと、本人確認に成功したことに応答して、第2の装置が、自分の秘密鍵で受信データ $E_b(N_a, S_a, Hash(S_a))$ を復号化して、セッション・キーの種 $S_a$ のハッシュ値



Hash' (S<sub>a</sub>) を計算して、受信したハッシュ値 Hash (S<sub>a</sub>) と一致するか否かによって、公開鍵における復号化に失敗したか否かを判別するステップと、復号化に失敗していないことに応答して、第2の装置が、相互認証用の乱数 N<sub>a</sub> を第1の装置に送信するステップと、第1の装置が、受信した乱数 N<sub>a</sub> が自分で生成した乱数と等しいか否かで第2の装置を本人確認するステップと、を具備することを特徴とする相互認証方法である。

【0028】ここで、CPUパワーが非力でメモリ容量が小さな携帯情報端末の相互認証を行うことを考慮して、NTRU公開鍵暗号方式を用いた相互認証処理を行う。

【0029】本発明の第2の側面に係る相互認証方法によれば、第1及び第2の装置は、通信相手を相互認証するとともに、お互いが正しく公開鍵で暗号化された乱数を復号化することができたか否かによって、復号化の失敗を起していないことを確認することができる。また、復号化の失敗を起していない場合のみ、互いに生成した種 S<sub>a</sub> 及び S<sub>b</sub> からセッション・キーを生成する。そして、その後のデータのやり取りを、セッション・キーで暗号化して送受信することにより、第3者による改竄や盗聴を防ぐことができる。

【0030】また、本発明の第3の側面は、通信媒体を介して接続される他の装置との間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証装置又は相互認証方法であって、相互認証用の乱数 N を発生する手段又はステップと、セッション・キーの種となる乱数 S を発生する手段又はステップと、セッション・キーの種のハッシュ値 H を計算する手段又はステップと、乱数 N とセッション・キーの種 S とセッション・キーの種のハッシュ値 H を通信相手の公開鍵で暗号化して送信する手段又はステップと、通信相手から受信した暗号データを自分の公開鍵で復号化して、通信相手の相互認証用の乱数 N' と通信相手が生成したセッション・キーの種 S' 及びそのハッシュ値 H' を取り出す手段又はステップと、セッション・キーの種 S' のハッシュ値 H'' を計算して、H' と H'' が一致するか否かによって公開鍵における復号化に失敗したか否かを検査する手段又はステップと、を具備することを特徴とする相互認証装置又は相互認証方法である。

【0031】ここで、CPUパワーが非力でメモリ容量が小さな携帯情報端末の相互認証を行うことを考慮して、NTRU公開鍵暗号方式を用いた相互認証処理を行う。

【0032】また、本発明の第3の側面に係る相互認証装置又は相互認証方法は、通信相手から受信した暗号データから取り出した通信相手の相互認証用の乱数 N' を通信相手に送信する手段又はステップと、通信相手から受信した自分の相互認証用の乱数が、自分で発生した乱

数 N と等しいか否かで、通信相手を本人確認する手段又はステップとをさらに備えていてもよい。

【0033】本発明の第3の側面に係る相互認証装置又は相互認証方法によれば、第1及び第2の装置は、通信相手を相互認証するとともに、お互いが正しく公開鍵で暗号化された乱数を復号化することができたか否かによって、復号化の失敗を起していないことを確認することができる。また、復号化の失敗を起していない場合のみ、互いに生成した種 S<sub>a</sub> 及び S<sub>b</sub> からセッション・キーを生成する。そして、その後のデータのやり取りを、セッション・キーで暗号化して送受信することにより、第3者による改竄や盗聴を防ぐことができる。

【0034】また、本発明の第4の側面は、他の装置との間で所定の公開鍵暗号方式を用いて相互認証を行うための相互認証処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、相互認証用の乱数 N を発生するステップと、セッション・キーの種となる乱数 S を発生するステップと、セッション・キーの種のハッシュ値 H を計算するステップと、乱数 N とセッション・キーの種 S とセッション・キーの種のハッシュ値 H を通信相手の公開鍵で暗号化して送信するステップと、通信相手から受信した暗号データを自分の公開鍵で復号化して、通信相手の相互認証用の乱数 N' と通信相手が生成したセッション・キーの種 S' 及びそのハッシュ値 H' を取り出すステップと、セッション・キーの種 S' のハッシュ値 H'' を計算して、H' と H'' が一致するか否かによって公開鍵における復号化に失敗したか否かを検査するステップと、を具備することを特徴とする記憶媒体である。

【0035】本発明の第4の側面に係る記憶媒体は、例えば、さまざまなプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で提供する媒体である。このような媒体は、例えば、CD (Compact Disc) や FD (Floppy Disk)、MO (Magneto-Optical disc) などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを經由してコンピュータ・ソフトウェアを特定のコンピュータ・システムに提供することも技術的に可能である。

【0036】このような記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、本発明の第4の側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発

明の第3の側面に係る相互認証装置又は相互認証方法と同様の作用効果を得ることができる。

【0037】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0038】

【発明の実施の形態】本発明は、NTRU Cryptosystems 社が発案した公開鍵暗号方式を使用した相互認証プロトコルを提案するものである。

【0039】NTRUは、因数分解や対数問題を使用しない、初の安全で実用的な公開鍵暗号システムである。NTRUのアルゴリズムを実行する計算プロセスは単純であり、低価格の8ビット・マイクロプロセッサでも高速に処理することができる。すなわち、NTRUの公開鍵暗号方式は、比較的軽い処理で且つ小メモリ容量で実現できることから、サーバとクライアント間、とりわけ、携帯電話機、デジタル・ミュージック・プレーヤや、PDAなどの携帯型のデバイスにおいて、例えば音楽などのコンテンツ配信サイトとの間での相互認証手続に適用することができる。

【0040】A. NTRU公開鍵暗号システム

ここで、NTRUの公開鍵暗号システムについて説明しておく。

【0041】NTRUの暗号化処理は、多項式代数、並びに、 $p$  と  $q$  2 個のレダクション・モジュロに基づく混合システムを用いる。一方、その復号化処理は、非混合システムを使用し、その有効性は基本的な確立理論に依存する。NTRUの公開鍵暗号システムのセキュリティは、多項式混合システムとレダクション・モジュロ  $p$  及

$$F \otimes G = H$$

$$\text{但し、} H_k = \sum_{i=0}^k F_i G_{k-i} + \sum_{i=k+1}^{N-1} F_i G_{N+k-i} = \sum_{i+j=k \pmod{N}} F_i G_j$$

【0048】NTRU鍵を生成するために、復号者側では2つの多項式  $f, g \in L_g$  を選択する。一方の多項式  $f$  は、モジュロ  $q$  とモジュロ  $p$  それぞれの逆数を持つという付加的な要件を満足する。ここで、それぞれの※

$$F_q \otimes f = 1 \pmod{q} \quad \text{and} \quad F_p \otimes f = 1 \pmod{p} \quad (1)$$

【0050】復号者側では次いで以下の量を計算する。 40★

【0051】

$$h = F_q \otimes g \pmod{p} \quad (2)$$

【0052】復号者側における公開鍵は上式で表される多項式  $h$  である。また、復号者側における秘密鍵は、多項式  $f$  である。但し、復号側では、 $F_p$  も併せて保管しておきたくなるのが実情である。

【0053】他方、暗号者側が復号者側にメッセージを送信したい場合、まず、平文の組  $L_m$  の中からメッセージ  $m$  を選択する。次いで、1つの多項式  $\phi \in L_\phi$  を

※  $q$  の独立性との相互作用によって導き出される。このセキュリティは、ほとんどの格子において、適度に短い場合とは反対に、極端に短いベクトルを探すことは極めて難しいという事実（実験的にも観察されている）にも依拠する。

【0042】NTRU暗号化システムは、 $(N, p, q)$  という3つの整数パラメータと、整数係数を持つ  $N-1$  等級の4組の多項式  $L_f, L_g, L_\phi, L_m$  で成り立つ。ここで、 $p$  と  $q$  は素数である必要はないが  $\gcd(p, q) = 1$ （最大公約数が1）であることと、 $q$  は常に  $p$  よりも相当大きな数であることを前提とする。ここで、下式で表されるリング  $R$  を導入する。

【0043】

【数1】

$$R = \mathbb{Z}[X]/(X^N - 1)$$

【0044】要素  $F \in R$  は、以下に示すような多項式又はベクトルで表現される。

【0045】

20 【数2】

$$F = \sum_{i=0}^{N-1} F_i x^i = [F_0, F_1, \dots, F_{N-1}]$$

【0046】また、リング  $R$  の乗算は記号“ $\otimes$ ”を丸囲みした演算子で表記される。この演算子は、巡回畳み込み積であり、例えば  $F$  と  $G$  の巡回畳み込み積は下式の通りとなる。

【0047】

【数3】

※ 逆数を  $F_q$  及び  $F_p$  とおくと、これらは下式のように表される。

【0049】

【数4】

$$F_q \otimes f = 1 \pmod{q} \quad \text{and} \quad F_p \otimes f = 1 \pmod{p} \quad (1)$$

★ 【数5】

ランダムに選択して、復号者側の公開鍵  $h$  を用いて以下の計算を行う。

【0054】

【数6】

$$e = p\phi \otimes h \pmod{q}$$

【0055】上式が暗号者側から復号者側に送信された



暗号化メッセージ  $e$  となる。

【0056】復号者側が、受信した暗号化メッセージ  $e$  を復号化したい場合には、自分の秘密鍵  $f$  を用いる（この復号化処理を効率的に行いたい場合には  $F_p$  を用いればよい）。

【0057】暗号化メッセージ  $e$  を復号化したい場合には、まず下式を計算する。

【0058】

【数7】

$$a = f \otimes e \pmod{q}$$

【0059】ここで、復号者は  $a$  の係数を  $-q/2 \sim q/2$  の範囲内で選択する。式  $a$  を整数係数を持つ多項式として取り扱うことにより、以下の式を計算することで元のメッセージを再現することができる。

【0060】

【数8】

$$F \otimes a \pmod{p}$$

【0061】以上説明してきたように、NTRU公開鍵暗号方式によれば、適切なパラメータ値を用いることにより、極めて高い確率で復号化処理により元のメッセージを再現することができる。しかしながら、パラメータの選択次第で、Decryption Failure を生じる可能性（すなわち、正確に復号化されないという可能性）がある。

【0062】B. 相互認証プロトコル

以下、図面を参照しながら、本発明の実施形態について詳解する。

【0063】本発明に係る相互認証プロトコルは、例えばサーバとクライアント間、とりわけ、携帯電話機、デジタル・ミュージック・プレーヤや、PDA（Personal Digital Assistant）などの携帯型のデバイスにおいて、例えば音楽などのコンテンツ配信サイトとの間での相互認証に適用することができる。

【0064】図1には、携帯端末に対してコンテンツ配信サービスを提供するネットワーク・システムの構成を模式的に示している。

【0065】同図に示すように、ネットワーク・システムは、インターネット11のような広域的なネットワークと、携帯電話機などの移動体に対してパケット通信などのサービスを提供する移動体通信網12と、その他の図示しないネットワークで構成される。移動体通信網12やその他のネットワークは、インターネット11に相互接続されている。

【0066】インターネット11上には、無数のサーバが存在する。このうちの一部は、音楽や画像などのコンテンツを有料で配信するコンテンツ配信サーバ13である。コンテンツ配信サーバ13は、アクセス・ポイントを介してインターネット接続されているパーソナル・コ

ンピュータなどの情報端末や、携帯電話機14を接続することで移動体通信網12経由でインターネット11にアクセスするPDAなどの情報端末15に対して、有料でコンテンツの配信サービスを行う。

【0067】〔従来の技術〕の欄でも既に述べたように、ネットワーク世界では顔が見えない相手とコンテンツの引渡しや対価の支払いなどの手続きを行なわなければならない。このため、コンテンツを無断複製や改竄などの海賊行為から保護したり、ユーザのプライバシーのなりすましによる侵害から保護しなければならない。

【0068】このため、本実施形態に係るネットワーク・システム上では、コンテンツ配信サーバ13がパーソナル・コンピュータや情報端末15に対してコンテンツ配信サービスを行う際に、相互認証手続きを採り入れている。また、携帯情報端末15の処理能力やメモリ能力を考慮して、処理が軽く且つ簡単なプロトコルで実装可能なNTRU公開鍵暗号方式（前述）を用いた相互認証を採用している。

【0069】図2には、本実施形態に係るネットワーク・システム上でのコンテンツ配信サービスの流れを概略的に示している。

【0070】まず、コンテンツ配信サーバ13は、取引相手となる携帯情報端末15と接続してセッションが確立すると（ステップS1）、相互認証並びにセッション・キーの生成を行う（ステップS2）。

【0071】次いで、コンテンツ配信サーバ13は、携帯情報端末15に対して課金処理を行う（ステップS3）。課金処理は、前ステップS2で生成されたセッション・キーを用いることで、安全な通信路を介して行うことができる。

【0072】次いで、コンテンツ配信サーバ13は、セッション・キーを用いてコンテンツ復号鍵を暗号化して、携帯情報端末15に送信する（ステップS4）。そして、注文を受けたコンテンツを暗号化してから、携帯情報端末15に送信する（ステップS5）。

【0073】これに対し、携帯情報端末15側では、受信したコンテンツ復号鍵をセッション・キーで復号化するとともに、このコンテンツ復号鍵を用いて受信した暗号化コンテンツを復号化する（ステップS6）。そして、コンテンツを再生して視聴して楽しむことができる。

【0074】なお、図2に示したフローにおいて、課金処理とコンテンツの配信処理の順番を入れ替えてもよい。

【0075】本実施形態では、CPUパワーが非力でメモリ容量が小さな携帯情報端末の相互認証を行うことを考慮して、ステップS2における相互認証処理にNTRU公開鍵暗号方式を用いたプロトコルを使用する。後述するように、本実施形態に係る相互認証プロトコルでは、通信相手が互いに乱数生成したセッション・キー用

10

20

30

40

50

の種を基にセッション・キーを作り出して、認証後のデータ送受信を暗号化して行うようになっている。

【0076】また、送信データ中にセッション・キーの種となる乱数とそのハッシュ値を加えることにより、Description Failureが起きているかどうかをチェックするようにした。この結果、Description Failureが起きているかどうかをチェックして、確かなセッション確立でセッション・キーを共有することができる。

【0077】図3には、コンテンツ配信サーバ13の機能構成を模式的に示している。同図に示すように、コンテンツ配信サーバ13は、インターネット11などのネットワーク経由でメッセージの送受信を行うための送受信部31と、携帯情報端末15などの外部の装置から受信した電子署名を検証する電子署名検証部32と、乱数生成部33と、サーバ13自身の電子署名を生成する電子署名生成部34と、送信メッセージの暗号化や受信メッセージの復号化を行う暗号処理部35と、発生した乱数やサーバ13自身の秘密鍵・公開鍵や通信相手の公開鍵など所定のデータを保存するメモリ部36と、認証処理部37と、配信コンテンツを蓄積するコンテンツ蓄積部38と、コンテンツ配信サービスを受けた外部の装置に対して課金処理を行う課金処理部39を備えている。

【0078】電子署名検証部32は、送受信部31で受信された携帯情報端末14の電子署名Certification Aを検証するとともに、この電子署名に含まれる携帯情報端末15の公開鍵E<sub>u</sub>を取り出して、メモリ部36に保存しておく。

【0079】乱数発生部33は、相互認証に用いられる乱数N<sub>u</sub>を生成したり、セッション・キーの種となる乱数S<sub>u</sub>を生成する。これらの乱数N<sub>u</sub>及びS<sub>u</sub>は、携帯情報端末15などの通信相手とセッションが確立している間はメモリ部36に保存されている。

【0080】電子署名生成部34は、コンテンツ配信サーバ13自身の公開鍵E<sub>s</sub>をメモリ部36から取り出して、このE<sub>s</sub>を含んだ電子署名Certification Bを生成して、送受信部31からコンテンツ配信先となる携帯情報端末15に送信する。

【0081】暗号処理部35は、携帯情報端末15などの通信相手に送信するデータを相手の公開鍵E<sub>u</sub>で暗号化したり、逆に携帯情報端末15から受信したデータを自分自身の秘密鍵で復号化したりする。また、暗号処理部35は、通信相手と交換し合った互いのセッション・キーの種を基にセッション・キーを生成して、認証処理後の送信データの暗号化に用いることができる。

【0082】認証処理部37は、携帯情報端末15などのコンテンツ配信先との間で認証処理を行う。例えば、通信相手からの受信メッセージに含まれるデータのハッシュ値を計算して、同じく受信メッセージに含まれるハッシュ値と照合することにより、通信相手が本物である

か否かを判別することができる。また、相互認証処理にNTRU公開鍵暗号方式を用いているが、認証処理部37は、ハッシュ値の照合により、Description Failureが起きているかどうかをチェックすることができる。

【0083】なお、コンテンツ配信サーバ13は、専用のハードウェア装置としてデザインすることも可能であるが、ワークステーション(WS)又はパーソナル・コンピュータ(PC)と呼ばれる一般的な計算機システム上で所定のサーバ・アプリケーションを起動させるという形態で実現することも可能である。

【0084】また、図4には、コンテンツ配信サーバ13からコンテンツの配信サービスを受ける携帯情報端末15の機能構成を模式的に示している。同図に示すように、携帯情報端末15は、携帯電話14経由でネットワークに接続してコンテンツ配信サーバ13との間でメッセージの送受信を行うための送受信部51と、コンテンツ配信サーバ13などの外部装置から受信した電子署名を検証する電子署名検証部52と、乱数生成部53と、携帯情報端末15自身の電子署名を生成する電子署名生成部54と、送信メッセージの暗号化や受信メッセージの復号化を行う暗号処理部55と、発生した乱数や携帯情報端末15自身の秘密鍵・公開鍵や通信相手の公開鍵など所定のデータを保存するメモリ部56と、認証処理部57と、コンテンツ配信サーバ13から受信したコンテンツを再生利用するコンテンツ再生部58と、コンテンツ配信サーバ13からの課金要求を処理する課金処理部59を備えている。

【0085】電子署名検証部52は、送受信部51で受信されたコンテンツ配信サーバ13の電子署名Certification Bを検証するとともに、この電子署名に含まれるコンテンツ配信サーバ13の公開鍵E<sub>s</sub>を取り出して、メモリ部56に保存しておく。

【0086】乱数発生部53は、相互認証に用いられる乱数N<sub>u</sub>を生成したり、セッション・キーの種となる乱数S<sub>u</sub>を生成する。これらの乱数N<sub>u</sub>及びS<sub>u</sub>は、コンテンツ配信サーバ13などの通信相手とセッションが確立している間はメモリ部56に保存されている。

【0087】電子署名生成部54は、携帯情報端末15自身の公開鍵E<sub>s</sub>をメモリ部56から取り出して、このE<sub>s</sub>を含んだ電子署名Certification Aを生成して、送受信部51からコンテンツ配信元となるコンテンツ配信サーバ13に送信する。

【0088】暗号処理部55は、コンテンツ配信サーバ13などの通信相手に送信するデータを相手の公開鍵E<sub>u</sub>で暗号化したり、逆にコンテンツ配信サーバ13から受信したデータを自分自身の秘密鍵で復号化したりする。また、暗号処理部55は、通信相手と交換し合った互いのセッション・キーの種を基にセッション・キーを生成して、認証処理後の送信データの暗号化に用いるこ

とができる。

【0089】認証処理部57は、コンテンツ配信サーバ13などのコンテンツ配信元との間で認証処理を行う。例えば、通信相手からの受信メッセージに含まれるデータのハッシュ値を計算して、同じく受信メッセージに含まれるハッシュ値と照合することにより、通信相手が本物であるか否かを判別することができる。また、相互認証処理にNTRU公開鍵暗号方式を用いているが、認証処理部57は、ハッシュ値の照合により、Description Failureが起きているかどうかをチェックすることができる。

【0090】図5には、携帯情報端末15とコンテンツ配信サーバ13間で行われる相互認証の処理手順の一例を示している。但し、携帯情報端末15は、NTRU公開鍵暗号方式による公開鍵 $E_a$ とこれに非対称な秘密鍵を持ち、同様に、コンテンツ配信サーバ13は、NTRU公開鍵暗号方式による公開鍵 $E_b$ とこれに非対称な秘密鍵を持つものとする。

【0091】まず、クライアントとしての携帯情報端末15は、自分の公開鍵 $E_a$ を含んだ電子署名CertificationAを送信する(P1)。

【0092】コンテンツ配信サーバ13側では、この電子署名CertificationAを受信すると、電子署名検証部32でこれを検証する。

【0093】電子署名が正しいと判断された場合には、乱数発生部33で、相互認証に用いる乱数 $N_b$ と、セッション・キーの種となる乱数 $S_b$ を発生させる。さらに、適当なハッシュ・アルゴリズムにより、セッション・キーの種 $S_b$ のハッシュ値Hash( $S_b$ )を計算する。そして、 $N_b$ 、 $S_b$ 、Hash( $S_b$ )を携帯情報端末15の公開鍵 $E_a$ で暗号化して、これを電子署名生成部34で生成した電子署名CertificationBとともに携帯情報端末15に送信する(P2)。

【0094】携帯情報端末15側では、電子署名CertificationBと暗号データ $E_a$ ( $N_b$ ,  $S_b$ , Hash( $S_b$ ))からなるメッセージを受信すると、相互認証とDescription Failureの検証を行う。

【0095】図6には、携帯情報端末15側で行われる相互認証とDescription Failureの検証を合わせて行うための処理手順をフローチャートの形式で示している。以下、このフローチャートに従って説明する。

【0096】まず、電子署名検証部52で電子署名CertificationBを検証する(ステップS11)。

【0097】電子署名が正しいと判断された場合には(ステップS12)、暗号化処理部55において、暗号化データ $E_a$ ( $N_b$ ,  $S_b$ , Hash( $S_b$ ))を復号化して、 $N_b$ 、 $S_b$ 、Hash( $S_b$ )を取り出す(ステップ

S13)。

【0098】次いで、復号化されたセッション・キーの種 $S_b$ に対して同じハッシュ・アルゴリズムを適用してそのハッシュ値Hash'( $S_b$ )を作成し(ステップS14)、これが受信データから取り出されたハッシュ値Hash( $S_b$ )と一致するか否かを判別する(ステップS15)。ハッシュ値が等しくなることによって、携帯情報端末15側ではDescription Failureが発生していないことを確認することができる。

【0099】再び図5に戻って説明する。Description Failureがないことが確認された後、携帯情報端末15では、乱数発生部53で、相互認証に用いる乱数 $N_a$ と、セッション・キーの種となる乱数 $S_a$ を発生させる。さらに、適当なハッシュ・アルゴリズムにより、セッション・キーの種 $S_a$ のハッシュ値Hash( $S_a$ )を計算する。そして、 $N_a$ 、 $S_a$ 、Hash( $S_a$ )を携帯情報端末15の公開鍵 $E_b$ で暗号化して、これを、相互認証用の乱数 $N_b$ とともにコンテンツ配信サーバ13に送信する(P3)。

【0100】コンテンツ配信サーバ13側では、乱数 $N_b$ と暗号データ $E_b$ ( $N_a$ ,  $S_a$ , Hash( $S_a$ ))からなるメッセージを受信すると、相互認証とDescription Failureの検証を行う。

【0101】図7には、コンテンツ配信サーバ13側で行われる相互認証とDescription Failureの検証を合わせて行うための処理手順をフローチャートの形式で示している。以下、このフローチャートに従って説明する。

【0102】まず、認証処理部37で、受信メッセージに含まれる $N_b$ が、乱数生成部33で生成した乱数 $N_b$ と等しいか否かを判別して(ステップS21)、通信相手が暗号化メッセージ $E_a$ ( $N_b$ ,  $S_b$ , Hash( $S_b$ ))から $N_b$ を取り出せたか否か、すなわち本物かどうかを確認する。

【0103】乱数 $N_b$ が一致すると判断された場合には、暗号化処理部55において、暗号化データ $E_b$ ( $N_a$ ,  $S_a$ , Hash( $S_a$ ))を復号化して、 $N_a$ 、 $S_a$ 、Hash( $S_a$ )を取り出す(ステップS22)。

【0104】次いで、復号化されたセッション・キーの種 $S_a$ に対して同じハッシュ・アルゴリズムを適用してそのハッシュ値Hash'( $S_a$ )を作成し(ステップS23)、これが受信データから取り出されたハッシュ値Hash( $S_a$ )と一致するか否かを判別する(ステップS24)。ハッシュ値が等しくなることによって、コンテンツ配信サーバ13側ではDescription Failureが発生していないことを確認することができる。

【0105】再び図5に戻って説明する。Description Failureがないことが確認された後、コンテンツ配信サーバ13は、復号化された乱数 $N_a$ を

10

20

30

40

50

携帯情報端末15に送り返す(P4)。

【0106】携帯情報端末15側では、受信したNaが乱数生成部53で生成したNaと等しいか否かを判別して、通信相手が暗号化メッセージE<sub>t</sub>(Na, Sa, Hash(Sa))からNaを取り出せたか否か、すなわち本物かどうかを確認する。

【0107】そして、上述したような手続により、携帯情報端末15及びコンテンツ配信サーバ13が通信相手を相互認証するとともに、自分自身がNTRU公開鍵暗号方式においてDescription Failure 10を起していないことを確認し終えたならば、交換し合ったセッション・キーの種Sa及びSbを併せてセッション・キーを作り出す。そして、課金処理や、コンテンツ暗号鍵の送信などは、このセッション・キーを用いた安全な通信路上で行うことができる。

【0108】2つのセッション・キーの種Sa及びSbを用いて、例えば以下の方法によりセッション・キーを生成することができる。

【0109】(1) Sa及びSbのXOR(Exclusive OR: 排他的論理和)値をセッション・キーとする。

(2) Saの上位バイトとSbの上位バイトを合わせたものをセッション・キーとする。

【0110】このような、各端末上で生成された種Sa及びSbからセッション・キーを生成することにより、お互いが正しく公開鍵で暗号化された乱数を復号化することができた場合(すなわち、Description Failureがない場合)にのみ、セッション・キーを作り出すことができる。

【0111】そして、その後のデータのやり取りを、セッション・キーで暗号化して送受信することにより、第 30 3者による改竄や盗聴を防ぐことができる。

【0112】図8には、携帯情報端末15とコンテンツ配信サーバ13間で行われる相互認証の処理手順に関する他の例を示している。但し、携帯情報端末15は、NTRU公開鍵暗号方式による公開鍵E<sub>a</sub>とこれに非対称な秘密鍵を持ち、同様に、コンテンツ配信サーバ13は、NTRU公開鍵暗号方式による公開鍵E<sub>b</sub>とこれに非対称な秘密鍵を持つものとする。

【0113】まず、クライアントとしての携帯情報端末15は、自分の公開鍵E<sub>a</sub>を含んだ電子署名Certification Aを送信する(P11)。

【0114】コンテンツ配信サーバ13側では、この電子署名Certification Aを受信すると、電子署名検証部32でこれを検証する。

【0115】電子署名が正しいと判断された場合には、乱数発生部33で相互認証に用いる乱数Nbを発生させ、これを携帯情報端末15側の公開鍵E<sub>a</sub>で暗号化して、これを電子署名生成部34で生成した電子署名Certification Bとともに携帯情報端末15に送信する(P12)。

【0116】携帯情報端末15側では、電子署名Certification Bと暗号データE<sub>a</sub>(Nb)からなるメッセージを受信すると、電子署名検証部32で電子署名Certification Bの検証を行う。電子署名が正しいと判断された場合には、暗号化処理部55において、暗号化データE<sub>a</sub>(Nb)を復号化して、Nbを取り出して、そのハッシュ値Hash(Nb)を作成する。さらに、乱数生成部53で相互認証に用いる乱数Naを発生させ、コンテンツ配信サーバ13側の公開鍵E<sub>b</sub>でこれを暗号化する。そして、このようにして作成されたE<sub>b</sub>(Na)及びHash(Nb)を含むメッセージを、コンテンツ配信サーバ13に送信する(P13)。

【0117】コンテンツ配信サーバ13側では、E<sub>b</sub>(Na)及びHash(Nb)を含むメッセージを受信すると、携帯情報端末15についての認証処理を行う。図9には、コンテンツ配信サーバ13側で行う携帯情報端末15についての認証手続をフローチャートの形式で示している。以下、このフローチャートに従って、携帯情報端末15についての認証手続について説明する。

【0118】まず、所定のハッシュ・アルゴリズムにより乱数発生部32で発生した乱数Nbのハッシュ値を計算する(ステップS31)。そして、計算されたハッシュ値が、携帯情報端末15から受信したハッシュ値Hash(Nb)と等しいか否かを判別する(ステップS32)。

【0119】これらハッシュ値が等しい場合、携帯情報端末15が正しくメッセージを復号化できたことを確認できるので、携帯情報端末15が本物の通信相手であることが判る。

【0120】次いで、受信した暗号化データE<sub>b</sub>(Na)を暗号処理部35で復号化して、携帯情報端末15側の乱数Naを取り出す(ステップS33)。

【0121】そして、所定のハッシュ・アルゴリズムによりこの乱数Naのハッシュ値Hash(Na)を計算して(ステップS34)、これを携帯情報端末15に送信する(ステップS35)(P14)。

【0122】また、コンテンツ配信サーバ13は、乱数発生部33で発生させた乱数Nbと、携帯情報端末15からの受信データを復号化して得られた乱数Naを基に、セッション・キーを生成する(ステップS36)。

【0123】携帯情報端末15側では、ハッシュ値Hash(Nb)を含むメッセージを受信すると、コンテンツ配信サーバ13についての認証処理を行う。図10には、携帯情報端末15側で行うコンテンツ配信サーバ13についての認証手続をフローチャートの形式で示している。以下、このフローチャートに従って、コンテンツ配信サーバ13についての認証手続について説明する。

【0124】まず、所定のハッシュ・アルゴリズムにより乱数発生部52で発生した乱数Naのハッシュ値を計 50

算する（ステップS 4 1）。そして、計算されたハッシュ値が、コンテンツ配信サーバ1 3から受信したハッシュ値H a s h（N<sub>a</sub>）と等しいか否かを判別する（ステップS 4 2）。

【0 1 2 5】これらハッシュ値が等しい場合、コンテンツ配信サーバ1 3が正しくメッセージを復号化できたことを確認できるので、コンテンツ配信サーバ1 3が本物の通信相手であることが判る。

【0 1 2 6】次いで、携帯情報端末1 5は、乱数発生部5 3で発生させた乱数N<sub>a</sub>と、コンテンツ配信サーバ1 3からの受信データを復号化して得られた乱数N<sub>b</sub>を基に、セッション・キーを生成する（ステップS 4 3）。

【0 1 2 7】図8からも判るように、上述した相互認証プロトコルによれば、コンテンツ配信サーバ1 3と携帯情報端末1 5間の通信路上では、セッション・キーの種となるN<sub>a</sub>及びN<sub>b</sub>なる乱数は、ハッシュがかけられた状態又は暗号化された状態でのみ現れる。したがって、仮に認証段階で通信路を傍受されたとしても、セッション・キーを推測されることは不可能である。また、コンテンツ配信サーバ1 3と携帯情報端末1 5は、一方から送られてきたハッシュ値と自分で作り出したハッシュ値が等しいことから、相手が正常に復号化できたことを確認することができる。

【0 1 2 8】2つのセッション・キーの種N<sub>a</sub>及びN<sub>b</sub>を用いて、例えば以下の方法によりセッション・キーを生成することができる。

【0 1 2 9】（1）N<sub>a</sub>及びN<sub>b</sub>のX O R（Exclusive O R：排他的論理和）値をセッション・キーとする。

（2）N<sub>a</sub>の上位バイトとN<sub>b</sub>の上位バイトを合わせたものをセッション・キーとする。

（3）N<sub>a</sub>とN<sub>b</sub>の和のハッシュ値H a s h（N<sub>a</sub> + N<sub>b</sub>）をセッション・キーとする。

【0 1 3 0】このような、各端末上で生成された種N<sub>a</sub>及びN<sub>b</sub>からセッション・キーを生成することにより、お互いが正しく公開鍵で暗号化された乱数を復号化することができた場合にのみ、セッション・キーを作り出すことができる。

【0 1 3 1】〔追補〕以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈すべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0 1 3 2】

【発明の効果】以上詳記したように、本発明によれば、音楽や画像などの有料コンテンツの配信において課金処理時に相互認証を好適に行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに

記憶媒体を提供することができる。

【0 1 3 3】また、本発明によれば、公開鍵暗号方式を用いて機器間の相互認証を好適に行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することができる。

【0 1 3 4】また、本発明によれば、比較的処理が軽い公開鍵暗号方式を用いて携帯端末のような組み込み機器のような資源が限られた機器環境でも相互認証を行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することができる。

【0 1 3 5】本発明によれば、N T R U公開鍵暗号方式を用いたプロトコルによりサーバとクライアント間の相互認証を行うことができる。また、このプロトコルで送受信されるセッション・キー用の乱数を基にセッション・キーを作り出して、認証後のデータ送受信を暗号化して行うことができる。また、N T R Uの公開鍵暗号方式は、復号化時に元のデータとは異なるD e c r i p t i o n F a i l u r eがあることが知られているが、送信データ中にセッション・キーの種となる乱数とそのハッシュ値を加えることにより、D e c r i p t i o n F a i l u r eが起きているかどうかをチェックできるようにして、確かなセッション確立でセッション・キーを共有することができる。

【0 1 3 6】したがって、本発明によれば、第3者によって見破られることがなく、安全にサーバとクライアント間の通信を行うことができる。例えば、E－C o m m e r c eなどにおける個人データ送信や、本人認証、課金システムなどに適用することができる。

【0 1 3 7】従来のS S L（Secure Socket Layer）などの相互認証プロトコルは、処理が重いため端末には不向きである。これに対し、N T R Uの暗号化方式は処理が軽いことや簡単なプロトコルであることから、携帯電話や携帯情報端末などの組み込み型機器に実装することが可能である。

【図面の簡単な説明】

【図1】携帯端末に対してコンテンツ配信サービスを提供するネットワーク・システムの構成を模式的に示した図である。

【図2】本実施形態に係るネットワーク・システム上でのコンテンツ配信サービスの流れを概略的に示したフローチャートである。

【図3】コンテンツ配信サーバ1 1の機能構成を模式的に示したブロック図である。

【図4】携帯情報端末1 5の機能構成を模式的に示したブロック図である。

【図5】携帯情報端末1 5とコンテンツ配信サーバ1 3間で行われる相互認証の処理手順の一例を示したフロー図である。

【図6】携帯情報端末1 5側で行われる相互認証とD e

cription Failureの検証を合わせて行うための処理手順を示したフローチャートである。

【図7】コンテンツ配信サーバ13側で行われる相互認証とDescription Failureの検証を合わせて行うための処理手順を示したフローチャートである。

【図8】携帯情報端末15とコンテンツ配信サーバ13間で行われる相互認証の処理手順に関する他の例を示したフロー図である。

【図9】コンテンツ配信サーバ13側で行う携帯情報端末15についての認証手続を示したフローチャートである。

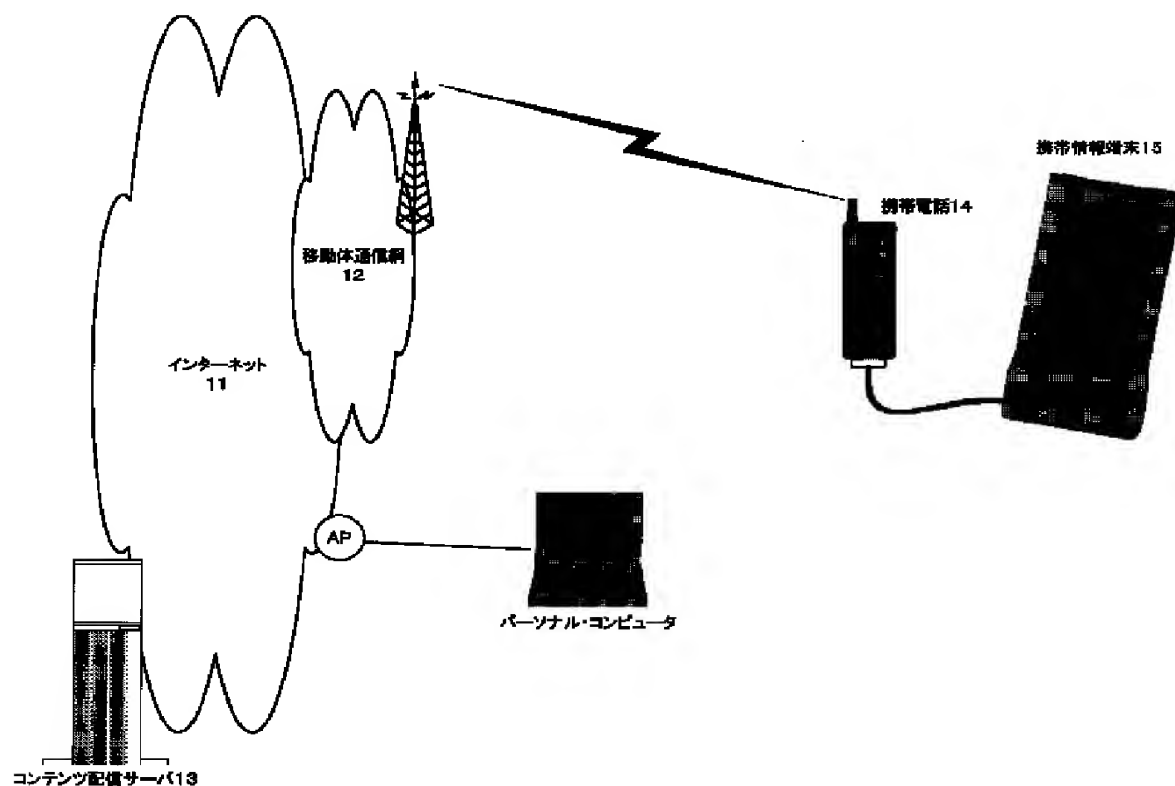
【図10】携帯情報端末15側で行うコンテンツ配信サーバ13についての認証手続を示したフローチャートである。

【符号の説明】

- 11…インターネット
- 12…移動体通信網
- 13…コンテンツ配信サーバ
- 14…携帯電話

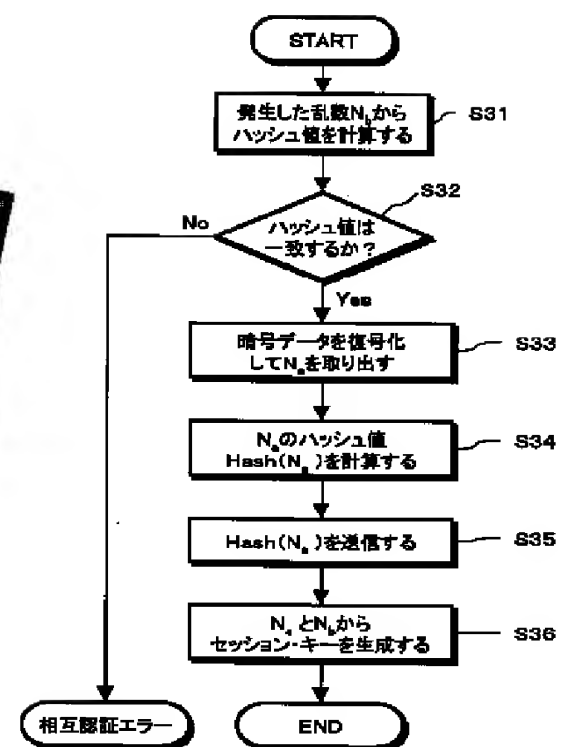
\*20

【図1】



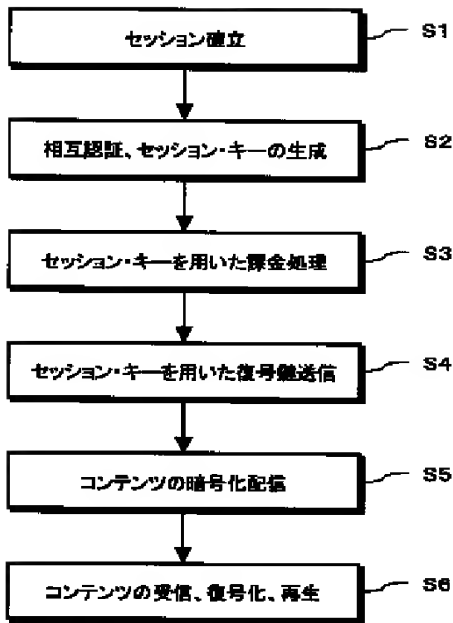
- \*15…携帯情報端末
- 31…送受信部
- 32…電子署名検証部
- 33…乱数生成部
- 34…電子署名生成部
- 35…暗号化処理部
- 36…メモリ部
- 37…認証処理部
- 38…コンテンツ蓄積部
- 39…課金処理部
- 51…送受信部
- 52…電子署名検証部
- 53…乱数生成部
- 54…電子署名生成部
- 55…暗号化処理部
- 56…メモリ部
- 57…認証処理部
- 58…コンテンツ再生部
- 59…課金処理部

【図9】

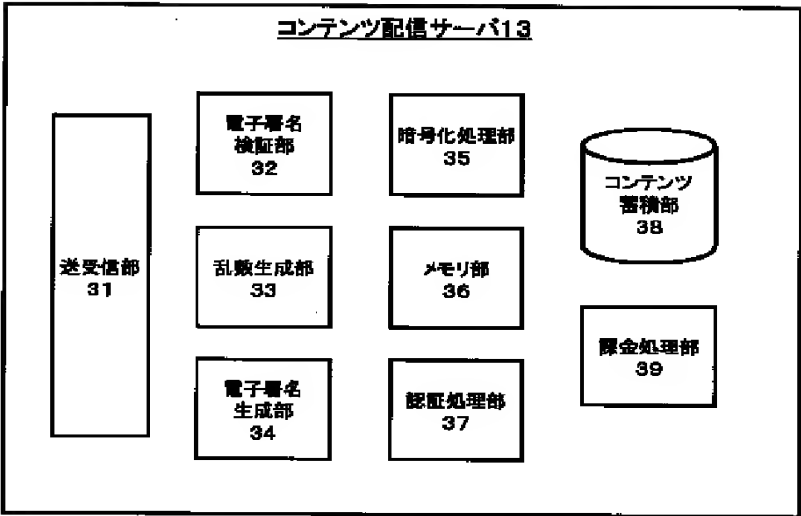




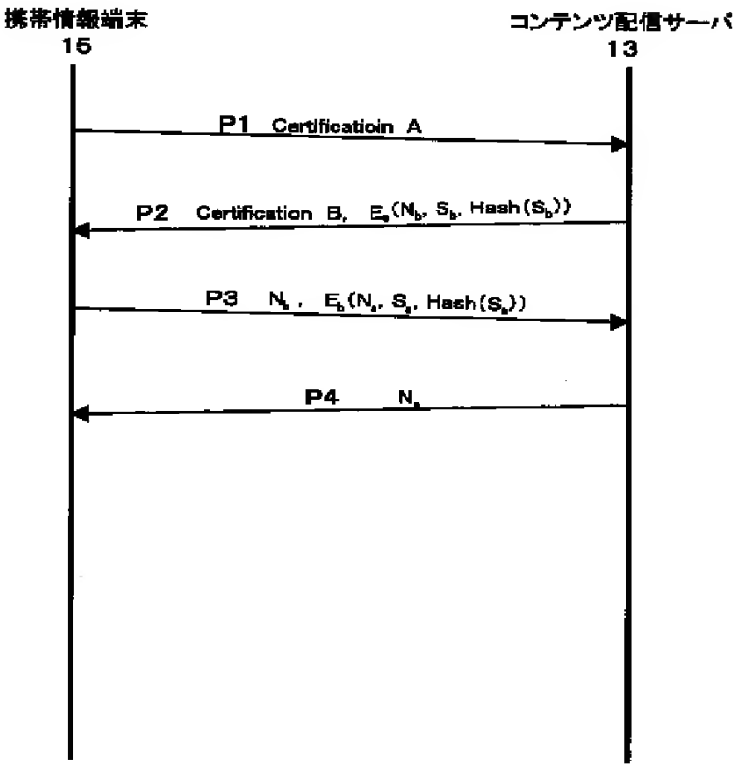
【図2】



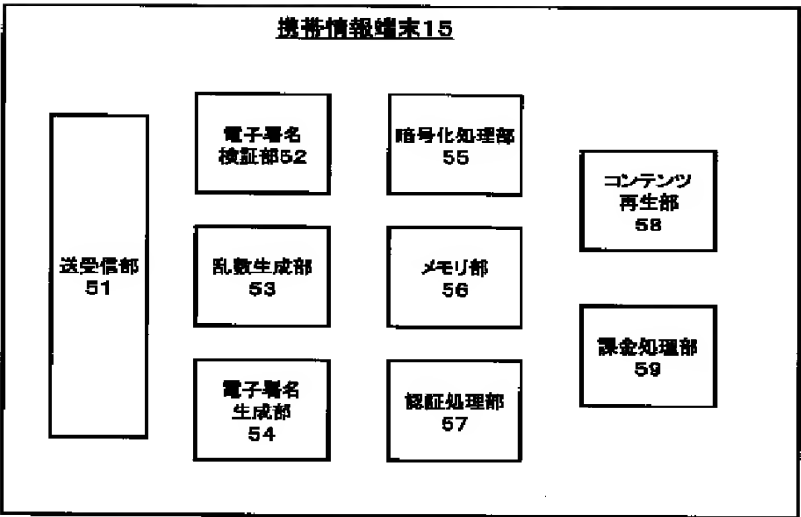
【図3】



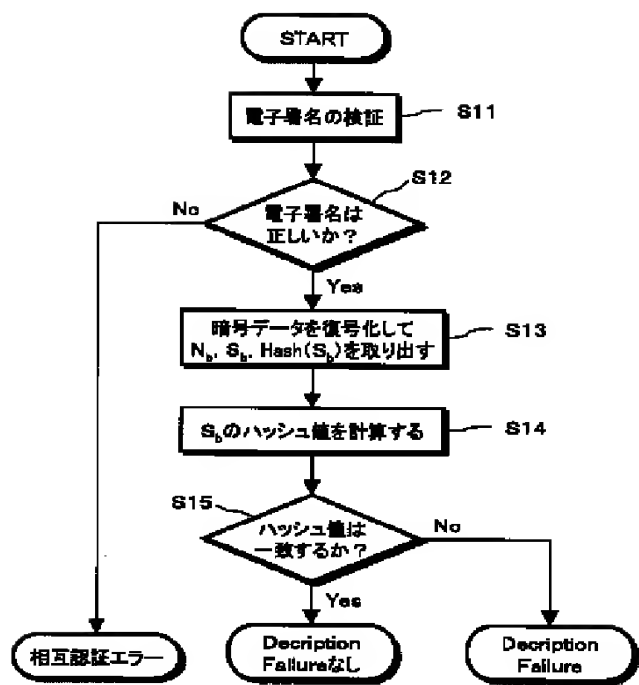
【図5】



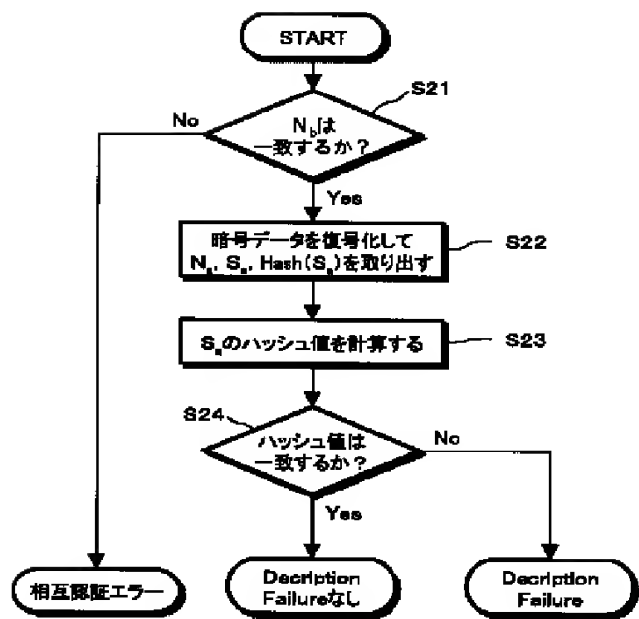
【図4】



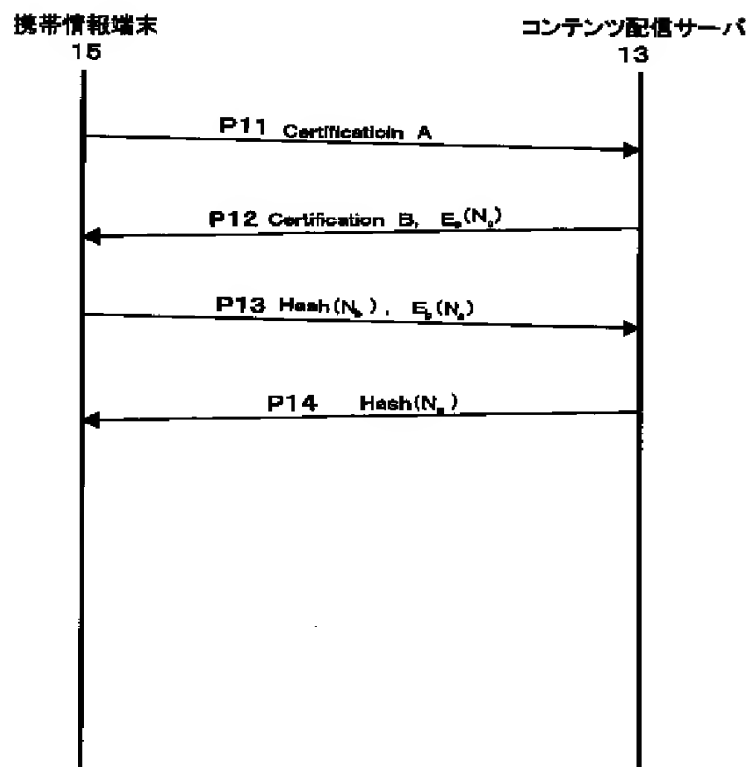
【図6】



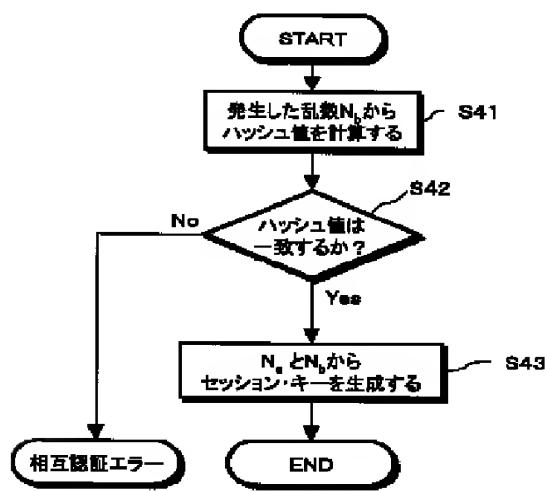
【図7】



【図8】



【図10】



フロントページの続き